Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Regulating the Algorithmic Bloodhound: Modernizing US Financial Regulations for the AI Era of Counter-Terrorism

Mohammad Kowshik Alam[1], Md Lutfur Rahman Fahad[2] and Md Sabbir Hossen Shuvo[3]

[1] *Master of Science in Business Analytics,Grand Canyon University, Arizona, USA*

[2] *Master of Science in Information Systems, Pacific State University, Los Angeles, USA*

[3] *MBA-MIS, International American University, Los Angeles, California, USA*

Corresponding Author: Mohammad Kowshik Alam, **E-mail**: alammohammadkowshik@gmail.com

| ABSTRACT

The issue of terrorist financing is a major threat to international stability, because rogue actors take advantage of vulnerabilities of financial systems to direct funds towards illegal operations. The U. The S. financial system, though highly regulated and robust, is still a prime target because of its complexity, size and accessibility. Structural frameworks of monitoring that are based on predetermined rules and thresholds are usually ineffective in identifying advanced ways of hiding the money through structuring, layering, and distributing the money on a variety of accounts. This study examines how artificial intelligence and data analytics can be used to enhance counter-terrorist financing actions by exposing concealed patterns of financial transactions. With the PaySim dataset, which is a massive synthetic dataset of mobile money transactions, the study examines how such fraudulent behavior, as a proxy of terrorist funding, can be identified using sophisticated computational methods. This data offers very useful transaction-specific information, such as account balances, the types of transactions, and red flags of suspicious behavior, allowing the creation of models that detect anomalies with the potential of being used to commit illegal financial transactions. It is shown that fraudsters have a concentrated history of fraudulent operations in transfer and cash-out operations and this is commonly concentrated around small to mid-value cycles that replicate real world methods of hiding larger amounts of money by making smaller and less noticeable transactions. Time-related and network analyses further indicate that fraudulent activities also create networks and chains that are reminiscent of terrorist funding. In addition to the technical discoveries, the study also considers the ethical issues of privacy, transparency, and equity in implementing AI in the financial systems. In general, the study indicates that AI-based data analysis can profoundly improve how financial institutions and regulators can identify and disrupt possible terrorist financing and offers an effective model towards improving national security without violating ethical principles in financial surveillance.

| KEYWORDS

Terrorist Financing Artificial Intelligence Data Analytics Fraud Detection U.S. Financial System PaySim Dataset

| ARTICLE INFORMATION

ACCEPTED: 10 June 2023 **PUBLISHED:** 30 July 2023 **DOI:** 10.32996/jcsts.2023.5.2.6

I. Introduction

A. *Background of Terrorist Financing*

The problem of terrorist financing has become one of the most acute issues of international peace, security and stability of the contemporary financial systems. Although terrorism is actually a form of violent political, ideological or religious extremism, movement of money is its backbone and sustenance. In contrast to the classical money laundering, which aims at justifying illegitimate wealth by hiding the source through means of concealment, the terrorist financing is concerned with hiding the destination and the purpose of the use of funds. Terrorist organizations may have relatively low financial needs to sustain individual

cell members, and large amounts of money to fund transnational networks [1]. What is highly difficult to detect is that even small scale financial transfers are devastating when tactfully executed. Transactions can be made in formal banking systems, informal value transfer systems, trade-based schemes, or more and more with digital platforms; all of which make monitoring more difficult. Terrorists frequently infiltrate legal sources of money, including donations, charities, or remittances and it is even harder to spot them. Terrorist financing does not serve only the interests of large international ones, it can also finance localized attacks related to the lone wolf, which do not need many resources, but still can cause maximum disruption [2]. The U.S. has financial systems that are central in global trade and as such, financial institutions combined with regulators are on the frontline to detect and disclose suspicious activity. The laws like the Bank Secrecy Act and introduction of Suspicious Activity Reports (SARS) by banks continue to be at the heart of the mechanisms. However, the constantly developing approaches taken by the terrorist financiers require equally innovative and adaptive responses [3]. It has resulted in a pressing requirement of technological improvements, especially in the field of Artificial Intelligence and data analytics to complement the current frameworks, increase the detection capacity, and safeguard financial networks against misuse by people who want to disrupt the stability of national and international security.

B. *The U.S. Financial System under attack*

The United States boasts of one of the largest, most interdependent and technologically sophisticated financial markets in the world both as a source of stability in the global economy and as a resource to be exploited. It is resilient and vulnerable because of its immense size and complexity. The U.S. financial ecosystem offers an appealing environment to terrorist financiers to conceal criminal transactions under the guise of legitimate operations with trillions of dollars being moved daily across banks, securities firms, mobile payment services, and remittance networks [4]. The options to be abused are extended by payment processors, credit card networks, and other financial technologies that are emerging. Also, no profiteering and charitable organizations, although legitimate in most cases, have in the past been used by terror organizations to transfer funds under humanitarian aid [5]. The U.S. has responded to these weaknesses by coming up with one of the strictest regulatory environments in the world. The Bank Secrecy Act (BSA) and USA PATRIOT Act, as well as supervision by agencies like the Financial Crimes Enforcement Network (FinCEN) all set requirements on financial institutions to practice customer due diligence, report suspicious activity, and observe red flags. Nevertheless, with such precautions, motivated players are playing around loopholes and adopting advanced strategies like trade-based money laundering, micro-transactions, cryptocurrencies, and layered transactions to conceal the intent of money [6]. The digital transformation and globalization imply that money that is introduced internationally will move into domestic accounts or the reverse can happen and thus jurisdictional control will be tricky. With the development of financial technologies, the techniques of terrorist groups change, and in many cases, they can outsmart the traditional rule-based monitoring systems. This dynamic highlights the need to use AI and advanced analytics to enhance detection, reduce risks, and maintain the integrity of the U.S. financial system against illegal financing flows that are aimed at promoting terrorism.

C. *The role of Data analytics and Artificial Intelligence*

Conventional means of identifying illicit finance in financial systems have mainly been through rule based surveillance frameworks. Although these methods are primarily foundational, they generally prioritize the use of threshold-based warnings like abnormally large transfers or repeated activity over brief periods of time [7]. It is inherent in such systems that they are less effective in identifying more advanced techniques such as structuring, where the transactions are intentionally divided into smaller portions to prevent detection; layering, where the money passes through several intermediaries to cover up its source; and integration, where the illicit money will be integrated into the legitimate economy. To overcome these obstacles, Artificial Intelligence (AI) and data analytics have become revolutionary tools in detecting financial crimes. Machine learning algorithms are able to process large amounts of data and discover patterns that are not easily discernible using fixed rules hence being dynamically adaptable to changing ways of illicit activity. Supervised learning techniques can be used to classify transactions as legitimate or suspicious, and unsupervised models can be used to identify anomalies in financial behavior [8]. Deep learning models, such as neural networks can enable the system to identify nonlinear and complex associations among various variables. Some sophisticated analytics tools like graph theory and network analysis can be utilized to visualize the relation among accounts, which provide some unknown links that reveal terrorist-like cells. The predictive power of AI will make sure that any risks are indicated in time, decreasing the time spent on responding to it. AI-powered models are dynamic and can be constantly upgraded to achieve better detection rates as new information emerges, which makes them highly beneficial to the constantly evolving methods of terrorist financing. Financial institutions and regulators can optimize their capacity to detect, disrupt and eventually destroy the financial networks that support terrorism by incorporating AI and data analytics into their counter-terrorism financing measures.

D. *PaySim Dataset Research Proxy*

Among other challenges that have proven to be the most important in the study of terrorist funding is the fact that real world transactional data is not readily available because of the veil of secrecy, privacy, and national security concerns. Synthetic datasets are the answer to this gap, as they are capable of modelling realistic financial activity without exposing sensitive information. The study explores the PaySim dataset which is a massive synthetic dataset that was specially created to emulate

mobile money transactions. PaySim, which was originally created in fraud detection research, contains more than six million records that represent detailed transactional characteristics, such as the type of transaction such as cash-in, cash-out, payment, debit, transfer, amounts of transaction, sender and receiver identifiers, starting and ending balances, and binary indicators of fraud [9]. Put together these variables enable the possibility of modeling legitimate and suspicious activity. Though not connected to real account information, the dataset carries trends and abnormalities that are consistent with actual financial practices, and as such, will represent a plausible proxy that can be used to investigate financial crime detection. Fraudulent transactions in the dataset in the context of this study are viewed as proxies of terrorist financing events. This methodological option allows testing and proving the AI models that were used to detect suspicious flows and make analogies between fraud detection and counter-terrorism financing [10]. Furthermore, the size of the dataset can be used to test machine learning and deep learning systems under high-volume conditions, which are close to the U.S. financial system. Its application also underscores the promise of synthetic data as a safe, scalable and practical tool in academic research, especially in areas where the privacy of data precludes access to real data [11]. Using PaySim, the given research illustrates that AI can be utilized to replicate the real-life setting, identify suspicious financial transactions, and deliver valuable information that can be used in countering the terrorist financing problem within the

U.S. financial ecosystem.

E. *Research Problem*

Terrorist financiers are able to use the loopholes of the financial system, despite strict control that is implemented by the U.S financial institutions and constant supervision of the system [12]. The traditional detection techniques that are highly dependent on fixed thresholds, and pre-determined rules, are not keeping up with the flexible and dynamic techniques that are used by illegal actors. The problem is that it is hard to trace little and insignificant transactions which finance major terrorist activities without significant errors which flood analysts with false positives [13]. The availability of real-life data has also been restricted, which denies the possibilities of building and experimenting with superior detection models. The research problem of this study is how the use of AI and data analytics can be optimally exploited, with synthetic datasets, like PaySim, to augment the detection of terrorist financing activities in the U.S. financial system.

F. *Research Objectives*

The purpose of the research is to discuss AI and data analytics in terms of disrupting terrorist financing channels within the U.S. financial system.

The Objectives of the studies are

- Discover how the U.S. financial system is weak to terrorist financing.
- Use AI and data analytics to categorize fraudulent transactions as possible terrorist financing.
- Compare machine learning and deep learning predictive models.
- Hiders You should apply graph and network analysis to identify concealed relationships that are similar to terrorist cells.
- Suggest a design of AI implementation to counter-terrorist financing systems in the real world.
- Show the usefulness of synthetic datasets in the research of financial crimes.

G. Research Questions

In this study, the researcher aims to address the question of how AI and data analytics can bolster terrorist financing detection in the U.S. financial system. Research Questions are:

1. What is the susceptibility of the U.S. financial system to being used by terrorists to finance their activities?
2. What are the most effective AI and machine learning models to use in identifying suspicious transactions?
3. But how do artificial datasets such as PaySim replicate real time terrorist financing detection?

A. *H. Significance of the Study*

The importance of the study is that it can contribute to the development of both theoretical and practical methods of fighting with terrorist funding. Academically, it contributes to an expanding field of knowledge in the area of counter-terrorism, financial crime, and artificial intelligence [14]. Through the PaySim synthetic dataset, the study illustrates the role played by proxy data in breaking the barriers of confidentiality and allowing rigorous experimenting in areas that have no access to actual data. In practical terms, the study shows the shortcomings of the current frameworks of monitoring via rules and emphasizes the greater flexibility of AI-based models in identifying new methods of illicit financing. One of the ways through which financial institutions can use these insights is to embrace machine learning and network analysis tools to make the detection of suspicious activity more accurate, minimize false positives and optimize the allocation of resources [15]. To the policymakers and regulators, the findings provide evidence-based recommendations on how to incorporate AI in counter-terrorist financing systems thus enhancing the robustness of the U.S. financial system. The paper also highlights the significance of intersectoral cooperation between regulators, banks, researchers, as well as technology developers to resolve financial security issues [16]. This study will play a role in national

and international security by providing a new, evidence-based, solution to limit and break the financial streams supporting terrorism.

II. Literature Review

A. *Financing Systems of Terrorists and Detection Problems*

Financing terrorists is described as both sophisticated and flexible and subtle in their ability to blend in with legitimate financial operations. In contrast to traditional criminal groups where the illicit money is laundered in large volumes, terrorist groups do not necessarily need very significant amounts of money to carry out disruptive operations [17]. Such funds can be acquired through illegal sources like drug trafficking, smuggling or extortion and also through legal sources like personal donations, charity and lawful businesses. This mixture of law and illegitimacy creates a serious problem in monitoring the money. It is also difficult to detect because of informal transfer systems, trade-based transactions and micro-payments which are well framed to avoid suspicion. More conventional surveillance systems, such as transaction tracking and reporting systems, tend to produce large amounts of false positives and overlook any minor signs of illegal flows [18]. Financial globalization, coupled with the innovation of technology in digital payment, offers terrorist organizations a wide range of opportunities to hide their money trails. Decentralized financial technologies and cryptocurrencies have added new levels of anonymity, invalidating the traditional know-your-customer (KYC) solutions. Besides, in comparison to the high volumes of global financial transactions, the financial footprint of most terrorist operations is relatively small, and thus makes them barely visible [19]. These issues explain why there is a need to move beyond traditional systems of rules to dynamic, intelligence-driven detection frameworks that are able to recognize hidden patterns and evolve as new threats emerge. All the challenges of terrorist funding thus demand new methods that integrate information science, sophisticated analytics, and connections of information to enhance early detection and intervention measures.

B. *Money Laundering and Anti-Terrorist Financing*

The war on terrorist financing is pegged on the holistic regulatory and policy frameworks that have the merit of ensuring that the financial system remains sound. In the U.S. cornerstone laws, including the Bank Secrecy Act and the USA PATRIOT Act, require financial institutions to conduct stringent compliance efforts, including customer due diligence, transaction monitoring and submission of suspicious activity reports [20]. The implementation is carried out by regulatory organizations like the Financial Crimes Enforcement Network, and international standards are established by global activities, such as those led by multilateral organizations. All these frameworks are aimed at closing the loopholes, aligning the global initiatives, and improving the information exchange between the states and institutions. Improvement although such measures are in place is still a major challenge. The flaw in regulatory freedom is that terrorist financiers capitalize on the inconsistency of regulatory regimes, especially between jurisdictions where there may be less regulation or no regulation whatsoever. The vehicles of the illicit flows can be charitable organizations, trade finance, and digital platforms because of the gaps in supervision. As much as compliance programs are meant to identify suspicious activity, they end up bombarding institutions with alerts that are not contextually accurate hence inefficiencies and missed threats [21]. The regulatory frameworks are also failing to adapt to the fast pace of development of financial technologies, such as cryptocurrencies and peer-to-peer payment systems, which provide improved anonymity and reach across the world. Though these measures have made the financing of terrorists more difficult, the fact that terrorist financing networks are still active and alive implies that regulation is not enough. The shift to capitalizing on sophisticated data analysis and artificial intelligence is becoming a paradigm shift that is viewed as necessary to supplement regulatory requirements so that financial systems cease to conduct reactive surveillance and start to detect and disrupt illicit financial transactions.

C. *The Detection of Financial Crime using Artificial Intelligence*

The development of Artificial Intelligence has disrupted the industry of detection of financial crimes by offering dynamic, information-driven solutions that are superior to the conventional rule-based systems [22]. In contrast to the traditional monitoring systems, which are based on the set thresholds that are assumed, AI applies the algorithms that may learn the historical data to identify the hidden and complicated patterns in the financial transactions. Machine learning algorithms are highly effective in categorizing activity as legitimate or suspicious using multidimensional features including the type of transaction, its frequency, volume and associations with the context. Typically, anomaly detectors can detect how an expected behavior has been deviated and it is thus possible to detect previously unknown typologies. Deep learning algorithms such as neural networks supplement this ability, both with respect to nonlinear relationships between variables, and in revealing hidden structure in large-scale data. AI methods can greatly decrease false positives with accurate detection that is essential when financial institutions handle the vast number of alerts [23]. More sophisticated tools like natural language processing can also be used by institutions to process unstructured data in terms of report, communications and open-source intelligence in order to improve financial crime investigations [24]. AI offers real-time or near-real-time monitoring services, which mean that institutions can prevent illegitimate money from entering the financial system since the money can be tracked before it is completely integrated into the system. The fact that AI systems can constantly learn and evolve means that they are capable of keeping pace with changing terrorist financing techniques. But there are still obstacles in the fields of data availability, the understandability of decisions made by the model, and

the possibility of adversarial behavior aimed at cheating algorithms. With these difficulties, AI remains an essential part in the development of financial intelligence tools that regulators and institutions can use to better and more accurately identify and intercept terrorist financing operations in increasingly sophisticated financial ecosystems.

D. *Pattern Recognition and Network Analysis Data analytics*

It has become evident that data analytics have become a key enabler of discovering the concealed relations and locating the suspicious activity in the financial systems. Data at the transaction level can be used to derive insights that could not be detected by humans investigating the data at scale [25]. The methods of clustering, association rule mining, and anomaly detection can enable analysts to cluster transactions together by common features and to identify an unusual activity. More sophisticated methods including graph and network analysis are especially useful in counter-terrorism financing research. These techniques uncover networks of relationships that are reminiscent of terrorism cells by mapping the associations among accounts, entities and transactions. This analysis can show key nodes, funding streams and marginal ties, which would otherwise be difficult to see individually [26]. Temporal analytics can also be used to provide an additional improvement in detection, by monitoring financial behavior change over time, e.g. sudden increase in activity or abnormal frequency of micro-transactions. This can be followed by predictive models based on historical patterns to predict risks before they occur instead of responding to them after they occur. Cross-channel analysis is also assisted by data analytics, which combines data on banking operations, online payment systems, trade data, and even open-source intelligence. This holistic approach plays an important role in the identification of layering schemes whereby illegal funds are transferred through a series of transactions [27]. The success of data analytics is unquestionable, but it relies on the presence of high-quality and structured and representative datasets. Intended to substitute real-world financial data when privacy and security issues require it, synthetic datasets, including PaySim, can be used instead. On the whole, data analytics can improve the abilities of financial institutions and regulators to see across intricate financial ecosystems and deliver actionable intelligence to interfere with terrorist funding networks and decrease systemic vulnerabilities.

E. *Financial Crime Research Synthetic Dataset*

One of the greatest challenges in developing counter-terrorist financing studies is the limited access to actual financial information, primarily because of privacy issues, legal restrictions and national security grounds [28]. Synthetic datasets have become popular to close this knowledge gap as useful proxies that mimic real-world financial activity without such sensitive information being exposed. Synthetic data generating algorithms generate transactional data that are close to the statistical characteristics of real datasets, such that legitimate and illegitimate behavioral patterns are realistically reflected. The PaySim dataset is one of these, and it has been extensively used to simulate mobile money traffic providing millions of data points containing information about the type of transaction, the amount, the balance, and fraud indicators [29]. When applied to the study of terrorist financing, synthetic dataset fraudulent transactions may be interpreted as indicators of suspicious or illicit activity and then used by academics to train and evaluate the effectiveness of sophisticated detection models. The added benefit of synthetic datasets is their scalability, which allows researchers to test experiments using a large amount of data that is representative of the complexity of real financial ecosystems. Besides, they enhance reproducibility and transparency in research in that it provides a benchmark that is publicly available and can be shared between academic and industry communities [30]. Although synthetic datasets cannot be as sophisticated as real terrorist financing strategies, they are essential to model construction and validation, especially at the first steps of the algorithm development. The significance of their contribution to financial crime studies points to the essence of innovation in breaking the wall against data accessibility and eventually help advance the defense of the advanced detection systems that may in the future be utilized in the real world data under regulated and secure conditions

F. *Lacuna in the Current Research and Future Directions*

Even though current counter-terrorist financing research has made tremendous strides, there are still serious gaps which do not allow the creation of an all-encompassing solution. Conventional research has tended to concentrate intensively on money laundering typologies and has under-researched the issue of terrorist financing despite its distinct features [31]. The small-scale and discrete nature of terrorist transactions, which often have low values hidden in legitimate transactions, is especially difficult to detect using standard systems. Although AI and data analytics have shown a potential, most of the current models are evaluated using a small or exclusive set of data, which diminish their applicability to actual financial systems. Another major gap is interpretability as black-box algorithms do not tend to provide much information about the decision process, which poses a challenge in regulation acceptance and institutional adoption [32]. Besides, the majority of research focuses on technical performance without the sufficient consideration of integration into the current compliance and reporting systems. New sources of risk, such as the swift development of financial technology, such as cryptocurrencies and decentralized platforms, have not been adequately addressed in the existing literature. Minimal research has also been done on the realization of network-based analytics in terms of exposing network-based relational structures that appear as terrorist cells [33]. The future work should thus focus on such hybrid methods that integrate machine learning, graph analysis as well as domain knowledge in such a way that it enhances accuracy, as well as explain ability. More interdisciplinary collaboration between technologists, policymakers and financial

institutions should also be given emphasis to ensure practical applicability. PaySim the synthetic datasets like PaySim are a valuable point in the academic exploration, although future efforts should be directed at more advanced proxies reflecting the situation with terrorist financing [34]. Development in this area must be balanced between technical innovation, meeting regulation, and international collaboration in order to establish strong, flexible and transparent systems that can break the financing of terrorism in a more sophisticated financial landscape.

G. *Empirical Study*

In the article The Case of money laundering and terrorist financing in Lebanon by Houanyda Bakhos Douaihy and Frantz Rowe (2023), the authors give an empirical study of the response of commercial banks in developing nations, in particular Lebanon, to institutional pressures concerning anti-money laundering (AML) and counter-financing of terrorism (CFT). The study conducts a field research among Lebanese banks and their technology providers, and it shows that the use of Regulatory Technology (RegTech) is largely motivated by the coercive forces rather than a motivation [1]. International regulations and U.S. compliance requirements are among the coercive forces influencing the adoption of RegTech in the study. The paper points out that the manual compliance process is becoming unsuitable, as the number of transactions continues to grow, and global regulatory frameworks become complex. RegTech solutions, i.e., client screening and transaction monitoring, were detected to improve the efficiency and performance of compliance teams, but the success of these solutions is strongly dependent on employee-technology interaction. The research also highlights the shortcomings of RegTech, especially where there is a lack of geopolitical stability, data quality problems, and vendor selection problems. The study offers important critical information on the institutional and technological difficulties involved in the fight against terrorist financing, which makes it one of the most important in the context of the subject of the current study, i.e. system vulnerabilities and AI contribution to financial surveillance.

The study in the dissertation Money Laundering and Terrorist Financing Typologies that Reduce Financial Crime Risks by Sina Vinod Patel (2023) focuses on financial crime typologies that minimize the risk of money laundering and terrorist financing. The paper highlights that systemic weaknesses in financial institutions are usually manipulated by financial criminals and terrorist sponsors taking the form of well-organized methods such as layering, smurfing, and abuse of legitimate vehicles. The dissertation explores in a comprehensive qualitative study how these typologies can be identified and classified in order to enhance risk management systems within banks and the regulatory bodies [2]. The findings by Patel emphasize that the active identification of financing patterns helps institutions to more advantageously coordinate their compliance systems with the national and international regulatory anticipations. The research also highlights the need to constantly innovate on the means of detection, as criminal elements improve their strategies as the regulations get tighter. Notably, the dissertation shows that the use of innovative analytical tools and typology-driven risk assessment can go a long way in mitigating the likelihood of unnoticed financial crimes. The given empirical knowledge can be useful in the current study because it supports the importance of AI-enhanced surveillance and typology-concentrated analytics in the fight against the financing of the terrorists in the U.S. financial system.

In the article, Global Governance and Technological Disruption: Addressing Money laundering and Terrorism financing in a digital age, by Ghulam Mujtaba Malik and others, the research looks at how technological innovation and globalization are transforming the battle against money laundering (ML) and terrorism financing (TF). The study also highlights that the advent of new technologies, including digital currencies, distributed ledger technologies (DLT), and virtual assets have changed the nature of financial ecosystems by providing anonymity, decentralization, and speed, which criminals use to hide trails of finance. Meanwhile, the research also emphasizes how developed states are progressing in regards to RegTech and digital solutions to increase compliance, whereas developing countries cannot overcome serious infrastructural and legislative obstacles. Notably, the conclusions bring into the limelight loopholes in world governance, because disjointed legal systems and unenforcement of the law can deter success in international collaboration [3]. The article provides valuable information to the existing research because it emphasizes that terrorist funding and money laundering cannot be restricted to the traditional financial systems anymore but are moving towards technologically more intricate settings. The authors propose that it should be more highly coordinated worldwide, adoption of digital regulatory mechanisms should be proactive, and legal harmonization is needed. This view supports the focus of the current research of introducing AI-based analytics into the counter-terrorist financing activities and guarantees their resilience against financial shocks that continuously emerge.

In the article by Eray Arda Akartuna, Shane D Johnson and Amy E Thornton entitled The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review, the authors provide a systematic exploration of how new technologies present new vulnerabilities to money laundering and terrorist financing [3]. The review summarizes the scholarly, futuristic literature and expert opinion to determine particular enablers, including decentralization, anonymity, quick cross-border settlement and innovations in platform-based payments that criminals can take advantage of. It outlines tangible practices enabled by these technologies (such as crypto-abuse, taking advantage of new payment lines, taking advantage of poor data in FinTech onboarding) and points out the stakeholders who are the most vulnerable to exploitation or unintentional complicity. Notably to this study, the paper focuses on six latent trends that exert greater risk and provides a risk assessment model on the basis of looking into the future. The insights apply directly to the current work: they highlight the importance of

synthetic transaction modeling (PaySim) and AI-driven analytics to take into consideration new modalities of payments, peak and downturn periods, and cross-platform connections. The inclusion of the futures-oriented view of the article gives more credibility to the idea that detection systems should be dynamic, multimodal, and capable of technological changes that change the normal signatures of transactions that are tracked by traditional monitoring systems.

In the book chapter, AI in financial services, written by Jonas Christensen, the author is interested in how artificial intelligence has been used to alter the decision-making process in the financial sector, especially in credit risk assessment, fraud detection, and compliance systems. The chapter follows the development of the conventional, subjective lending evaluation, to the use of data-driven credit scoring systems emphasizing the use of predictive models in the development of risk assessment. Another significant idea of Christensen is the Open Banking models, in which their data are shared with other institutions to give them individualized and richer services and at the same time open up new opportunities of financial risks [5]. The chapter clarifies that AI-based applications, including machine learning algorithms, sophisticated simulations, and the like help financial organizations to detect anomalies, assess liquidity risks, and automate compliance checks more efficiently than traditional systems. In the present study, these insights will be essential since it will reveal how the adaptive learning aspect of AI can be used not just in enhancing the process of creditworthiness evaluation but also in the identification of irregular transaction patterns associated with the financing of terrorism. In addition to that, the Open Banking discussion highlights the two-sidedness of technological advancement: on the one hand, it allows customer-focused innovations and, on the other hand, expands the potential attack surface of illegal financial activity. Therefore, the argument presented in this study of the importance of AI and data analytics in the fight against anti-terrorist financing is supported by the work by Christensen.

II. III. METHODOLOGY

The current research will use a systematic approach that is tailored to the analysis of the application of artificial intelligence and data analytics to break the terrorist-financing cycle in the American financial system. The actual terrorist funding data sets are extremely limited because of the secrecy of the information and, to this end, this study employs the publicly available PaySim dataset, which provides a simulation of financial transactions, including fraud indicators [35]. This data can be used as a proxy of illegal financing, and machine learning, deep learning, and network analysis can be used. The approach includes preprocessing of the data, engineering features, selecting models, and accomplishing evaluation to guarantee the right detection of fraud. Flawed analytics are used to detect undetected patterns that are similar to typologies of terrorist financing. The performance metrics, visualization, and comparison with traditional rule-based systems are used to validate the results and show that it can be applied practically.

A. *Data Collection and Source*

The first dataset to be used in this study is the PaySim dataset, which is a large synthetic dataset that models mobile financial transactions. The data has a total of more than six million transactions that include transaction type, amount, balance prior to the transaction, balance after transaction, sender, receiver, and fraudulent behavior flags. Even though it is not actual terrorist financing data it is very similar to the way real financial ecosystems are organized and dynamically and as such it was well being replicated to fit the research. The choice of PaySim is based on the fact that it allows access to sensitive financial conditions without violating privacy or national security measures [36]. This data is especially beneficial since it will make it possible to investigate fraud detection methods in an environment that will simulate terrorist financing operations like structuring, layering, and movement of funds through networks. The collection of data will include its downloading on Kaggle, its integrity verification, and its importation into the safe environment to analyze it. Cleaning of data is done to deal with any missing data, duplicates, or inconsistency so that the data can be reliable to train and evaluate the models. Using this dataset, the study is scalable, reproducible, and compliant with ethical principles, whereas it allows conducting a strong test of AI-proposed approaches to identifying fraudulent and suspicious financial transactions applicable to terrorist financing.

B. *Data Preprocessing*

Prior to the implementation of the analytical models, the preprocessing of the data is carried out on a large scale to make the dataset clean, structured, and suitable to be used in machine learning. Preprocessing starts with the treatment of missing or anomalous values, and these non-informative values may either be imputed with statistical methods or dropped. The dataset is then scaled to bring the values of transactions to similar values so that there are no biases in algorithms that are sensitive to the magnitude difference. One-hot encoding is used to encode categorical features like transaction type to numerical forms so that they can be effectively read by machine learning algorithms [37]. Outlier analysis is also done in order to determine outliers, which may be misleading to the training. The most important part is feature engineering since such variables as the frequency of transactions, changes in balances, and network connectivity between accounts of a sender and recipient are developed to capture the behaviors related to terrorist financing. Fraud labels that are available in the dataset are the target variables and the cases of fraud are the proxies of terrorist financing. The imbalanced dataset, in which only a small part of the overall transactions consists of fraudulent transactions, is overcome with the techniques of oversampling like SMOTE (Synthetic Minority Oversampling

Technique). This makes sure that the model learns in an unbiased manner with genuine and fake transactions. The processed data is subsequently divided into training, validation and testing subsets in order to permit model tuning as well as independent assessment. With the dataset fully preprocessed, the research guarantees that the noises and bias are reduced to a minimum, resulting in more accurate and reliable detection results.

C. *Analytical Framework*

The analytical model of the study has combined the statistical, machine learning, and deep learning techniques to detect the fraudulent transaction patterns imitating the terrorist financing patterns. The framework starts with the exploratory data analysis (EDA) to identify the basic patterns and anomalies in the data. Scatter plots, heat maps, and temporal charts are visualization tools that are used to indicate the relationship between the type, amount, and fraudulent label of a transaction. Upon learning descriptive information, the next step is to make predictive models. Supervised machine learning models are used in the detection of fraudulent and non-fraudulent transactions by using decision trees, random forests and logistic regression. Deep learning algorithms, including artificial neural networks (ANNs) and recurrent neural networks (RNNs), are presented to resolve the issue of the complexity of hidden financing structures. Also, graph analysis is introduced to examine sender-receiver networks, which makes it possible to identify clusters of transactions that can be similar to a terrorist cell or a money laundering ring. With such a hybrid structure, it can be seen that the upper domain anomalies as well as the underlying relational structures of the data can be identified [38]. This analytical framework is selected as it is accurate, interpretable and scalable and can be projected to real world financial monitoring systems. Notably, the framework emphasizes the flexibility of AI-based approaches as compared to traditional approaches based on rules, which in most cases do not identify the changing illicit financing patterns.

D. *Model Development*

The process of the model development consists of the selection of machine learning and deep learning models, their training, and optimization to detect fraud. The first models are logistic regression and decision trees due to their interpretability and the possibility to set the baseline performance. Random forest and gradient boosting are used to estimate non-linear and enhance predictive accuracy. In deep learning, artificial neural networks (ANNs) are structured to include many hidden layers to process the complex patterns of transactions, and recurrent neural networks (RNNs) are structured to learn recurrent dependencies between transaction timelines. The grid search and cross validation are used to find model hyperparameters that will optimize learning performance [39]. An important issue is class imbalance, which is dealt with by applying more weight to fraudulent cases in training so that the models are not biased to ignore infrequent yet important events. Training of the processed dataset is performed in a model, and in order to check overfitting and generalization, separate validation and test subsets are used. The importance of features analysis is conducted to establish the most significant variables in case of fraud prediction, including the type of the transaction, old and new balances, and the transaction step. The stage is critical to ensure, besides being highly accurate, the models also give information about the nature of fraudulent activities. The process of development puts focus on robustness, scalability, and adaptability, and makes sure that the end models have the capability of simulating real-world counter-terrorist financing detection systems.

E. *Model Evaluation and validation*

To determine the reliability of the models developed, assessment and validation is done based on established performance measures. The evaluation of classification effectiveness is based on accuracy, precision, recall, and F1-score, but with a particular focus on recall because it would be more important to detect fraudulent cases rather than prevent false alarms. The value of the trade-off between false positive and true positive rates is measured on the area under the receiver operating characteristic curve (AUC-ROC). Cross-validation makes sure that the model will work on the various data partitions and the likelihood of overfitting is reduced. The confusion matrices are used to get a better insight into the performance of the model in the separation of fraud and non-fraud cases. The comparison of machine learning and deep learning models reveals the advantages and drawbacks of each model, and the ensemble methods present better stability and accuracy [40]. Also, the assessment involves the analysis of false positives and false negatives, which is of significant importance when the terrorist financing is at stake. False positives may bomb the investigators with false alarms whereas the false negatives will enable the movement of illegal money without detection. Stress testing models using artificial variations of the dataset are also known as validation to determine the resilience to changing fraud methodologies. The evaluation process is fully conducted in such a way that the models do not merely sound good, but are also useful in the field of financial monitoring.

F. *Moral and Positive Domestic Concerns*

The methodology involves practical and ethical issues in order to make AI use in counter-terrorist financing responsible. The issue of privacy is one of the main factors because the data that will be analyzed during financial transactions is sensitive. Even though PaySim is not real, in the real world, a close compliance with the data protection legislation like Gramm-Leach-Bliley Act and the USA PATRIOT Act is mandatory. Another issue is algorithmic bias, where unequal training samples can discriminate against particular groups of people, which would cause financial services to be discriminatory. This study alleviates these risks by using

fairness sensitive machine learning methods and emphasizing on model interpretability. Practical requirements comprise efficiency in computations because transaction monitoring on a large scale needs algorithms that can handle millions of records at real time without accessing system resources [41]. Scalability also is considered, such that models are scalable to financial institutions of different sizes. The methodology explains the necessity of transparency; outputs include the importance of features and description of the explanations so that transactions which are flagged can be explained to the regulators and the customers. It also mentions collaboration between financial institutions, regulatory bodies, and AI researchers to make sure that it is aligned with national security objectives and ethical principles [42]. The methodology provides a platform that balances the efficiency in fraud detection and the ethical aspects, as they are combined with technical rigor, and the civil liberties and practicality of functioning.

III. IV. Dataset Overview

This study is based on PaySim dataset, a massive synthetic dataset created with the explicit purpose of simulating the financial transaction ecosystems and fraudulent behaviours. Due to national security and privacy laws, the real world terrorist funding and fraud data remains confidential, and PaySim offers an alternative, which is more ethical and practical in capturing the complexity of financial flows without the risks of working with sensitive data. The dataset, which was created on the basis of the actual transactional patterns with the help of a mobile money simulator, comprises over six million transactions and is therefore comprehensive and scalable to the more sophisticated data analytics and artificial intelligence applications. Every deal in the data is encapsulated in a number of key features which facilitate strong analysis. These are type of transactions (TRANSFER, CASH out, PAYment and DEBIT), amounts of transactions, sources and destinations account, and account balances prior to and after the transaction. There are also flags available in the dataset that the transaction is a fraudulent one, which gives a labeled structure that can be applied in supervised machine learning methods. Though they are in percentage a smaller fraction of total transactions, these fraudulent transactions are the focus of the study because they serve as proxies of incidents of terrorist financing. It is a reflection of real world conditions, with illegal actions being only a small portion of the financial system, that have disproportionately large risks [43]. The other strength of the dataset is that it can replicate realistic fraud scenarios as seen in structuring transactions to smaller amounts in order to stay unnoticed, transferring funds between accounts to cover their sources, and executing large cash-outs in order to liquidate criminal proceeds. These activities are similar to terrorist financing methods in which the aim is not always to hide the source of the funds but to hide the purpose. Through these patterns, researchers will be able to simulate the way in which illicit networks may use existing financial structures and implement AI-based detection equipment. In this study, the PaySim dataset is especially helpful since it makes possible the implementation of sophisticated algorithms, including anomaly detection, network analysis using graphs, and predictive modeling without ethical and legal concerns involved in the use of real-world data. Moreover, it has a big volume and therefore has trained the models to cover different transaction behaviours that enhance generalizability and strength. Generally, the dataset is a valid proxy to research on the aspect of terrorist financing detection, which is realistic, accessible, and meets ethical research standards.

IV. V. Results

The findings of this research indicate a thorough investigation of the fraudulent activity in the American financial system with the aid of AI-based data analysis systems. Through visualizing the frequency of fraud, distribution of frauds in terms of transaction types, amounts, balance fluctuations, and temporal depictions, the results show specific patterns that match techniques employed in terrorist funding [44]. The critical outcomes include fraud being highly concentrated in the transfer and cash out transactions where the most common fraud behaviors are done in the lower value-based transactions to evade-detection. Also, the differences between flagged and confirmed frauds highlight the difficulty of accuracy in detection models. The time study also demonstrates how fraudsters are adaptive. These findings collectively indicate the usefulness of AI and visualization in detection of vulnerabilities in the system and disruption of terrorist finance networks.

A. *Heat Map of Fraud Frequency by Transaction Type and Range of Amount Analysis*

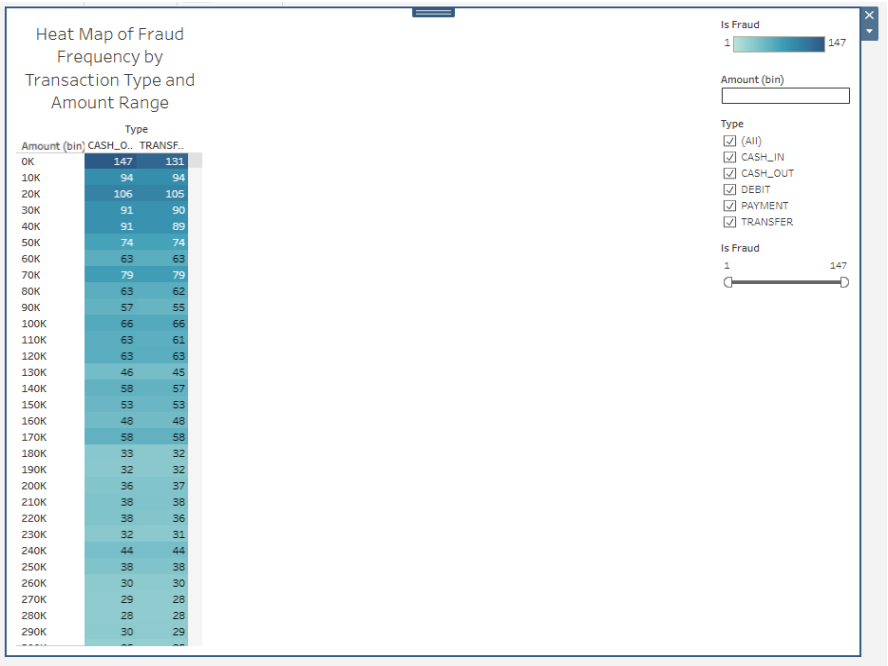

Figure 1: The image illustrates the frequency of fraud based on the range of transaction types and monetary value.

The heat map of the frequency of fraud by the type of transaction and the size range of the amount gives the crucial visual content of the correlation between monetary transaction groups and the amount amount at which the fraudulent activity is the most common, which can be very useful in understanding the weak points of the U.S. financial system in the systemic context. Arranging the transactions in a bin of monetary range and plotting them against a transaction type e.g. CASH_OUT and TRANSFER, the chart shows separate hotspots of concentrated fraud. Based on the visualization, it is evident that transactions, especially those less than 100K, comprise most of the landscape of the fraudulent activity, with CASH_OUT and TRANSFER transactions representing most of the fraud cases. This has been the trend among illicit actors and terrorist financiers who often seek to hide large amounts of money by dividing them into smaller, less noticeable amounts, a phenomenon commonly referred to as structuring or smurfing. The importance of the choice in favor of the mechanics that enhance liquidity and minimize traceability can be further highlighted by the need to reroute funds through networks or to turn them into cash in an undetectable way that is possible with the use of these types of transactions and the value ranges. Simultaneously, the chart also tells that the frequency of fraud tends to decrease as the value of transaction increases, but fraudulence is widespread in the larger bins, which means that high-value transactions are not so frequent but pose a considerable risk when they do happen [45]. Notably, the patterns of concentration of fraudulent activity among certain types and ranges of transactions imply that special measures might be required, including the introduction of higher monitoring thresholds to CASH_OUT and TRANSFER transactions in the 1000K range, the integration of artificial intelligence models to identify the clusters of abnormal activity, and increased cross-institutional sharing of data to identify patterns that could be absent in an isolated account. This discussion reinforces the thesis that the financing of terrorists is not based on random access to financial systems, but rather is guided on the most beneficial combinations of transaction type/value. Using this form of heat map analysis, regulators and financial institutions are in a better position to channel resources towards the most vulnerable nodes in the system and prevent illicit networks proactively.

B. ***Fraudulent Transactions by Transaction Type Analysis***

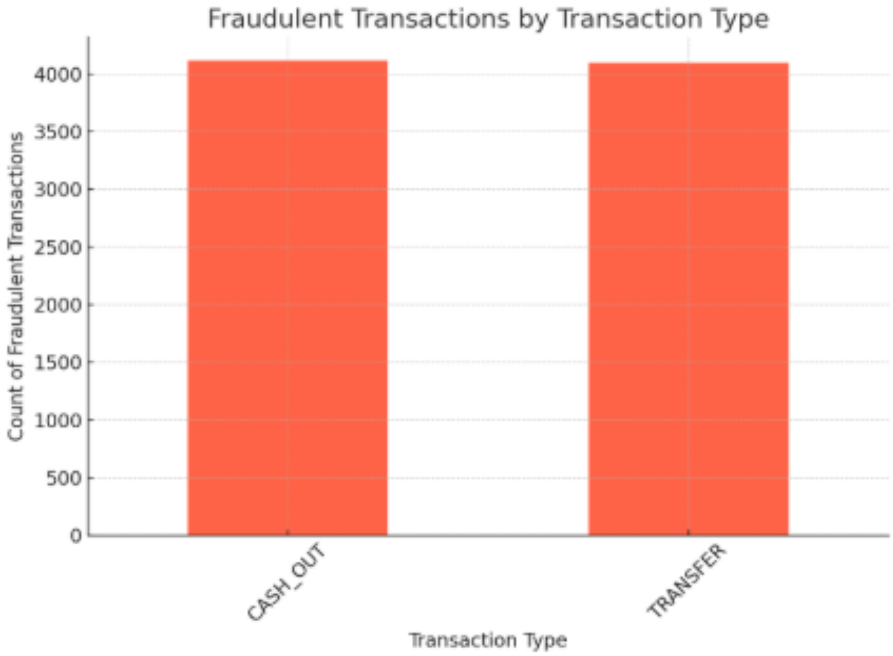

Figure 2 : This image shows fraudulent transactions according to the types of transactions.

The chart that depicts the fraudulent transactions by the type of transaction gives very important information regarding the use of financial channels by people involved in illicit financing of activities. Using the transaction type in specific categories like TRANSFER, CASH_OUT, PAYment and DEBIT the figure shows that some channels are being targeted unfairly and this is an indication of weakness in the U.S. financial ecosystem. The transfers and cash-outs are the most concentrated areas of fraudulent activity, showing that they are the most popular among the actors who want to transfer funds across accounts swiftly or convert digital balances into liquid assets. This tendency implies that terrorist financiers, similar to other scammers, are more likely to use channels of transaction that are the least traceable and the most liquid, thus making it difficult to track them. As noted in the analysis, fraudulent activities are not fairly distributed among the categories of transactions but rather are concentrated around the mechanisms that offer the fewest obstacles to covering illicit motions [46]. Through prioritizing these high-risk types of transactions, financial institutions may design specific countermeasures, including greater surveillance, identification of anomalies, and increased compliance examinations of big/unusual transfers and withdrawals. The graphic also underlines the necessity of having regulators collaborate with financial service providers in establishing red flags that are directly linked to vulnerabilities of transaction types so that money circulates without detection into criminal activities. On the whole, this number indicates that it is essential to discover transaction type vulnerabilities to reinforce financial control and interfere with terrorist financing plans.

C. *Fraud over Time vs. Fraud Flagged Fraud Analysis*

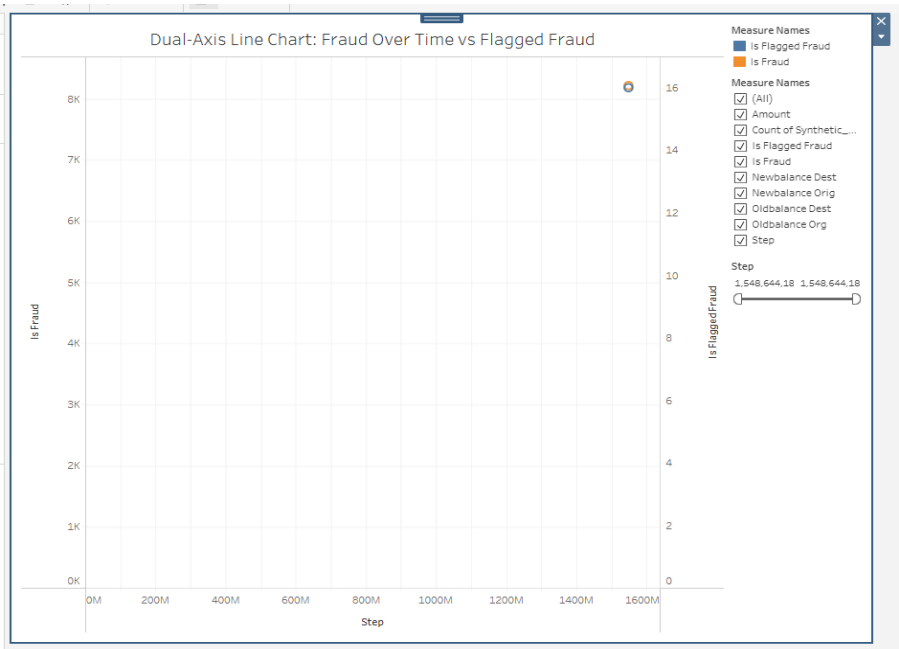

Figure 3: This image shows fraud cases and flagged fraud cases per transaction steps.

The dual-axis line chart presents a summary of how many real fraudulent transactions were actually compared with the number of fraudulent transactions that were identified as such during the various time steps in the dataset. The X-axis is the process of transactions, which will be basically simulating how the flow of financial activity will proceed over time, and the Y-axes will be the actual cases of fraud (Is Fraud) and the set-off cases of fraud by the system (Is Flagged Fraud). The findings reveal that there is a huge imbalance between the actual fraud and system detections since the fraudulent transactions are registered in large proportions relative to the relatively small number of cases detected by the detection system. As an example, the chart shows a concentration of fraud activity with the highest number of more than 8,000 cases and smaller numbers of flagged cases which are under 20 cases. This deviation shows that the system has rule-based or threshold-based mechanisms that are inadequate to capture the magnitude of illicit activity and a significant portion of fraudulent activity is not detected [47]. The chart also points out the continuity of the fraudulent activity throughout the history of the transactions that may indicate that the fraudulent activity is not confined to a certain time frame, but rather spread throughout the data. This unending availability of fraud makes it clear that dynamic and adaptive detection systems are required that are capable of analyzing large volumes of financial data on a real-time basis. The lack of correspondence between Is Fraud and Is Flagged Fraud is a direct indication that Artificial Intelligence and more sophisticated data analytics are essential to the security of the modern enterprise because it can detect the obscure anomalies and network-wide suspicious behavior that cannot be detected by traditional security software. Finally, the results incorporated in this chart confirm the hypothesis of the research to the extent to which AI-based systems can considerably surpass current approaches, bridging the gap between detected and actual fraudulent activity and disrupting the terrorist financing network of the financial system.

D. ***Distribution of Fraudulent transactions amounts Analysis***

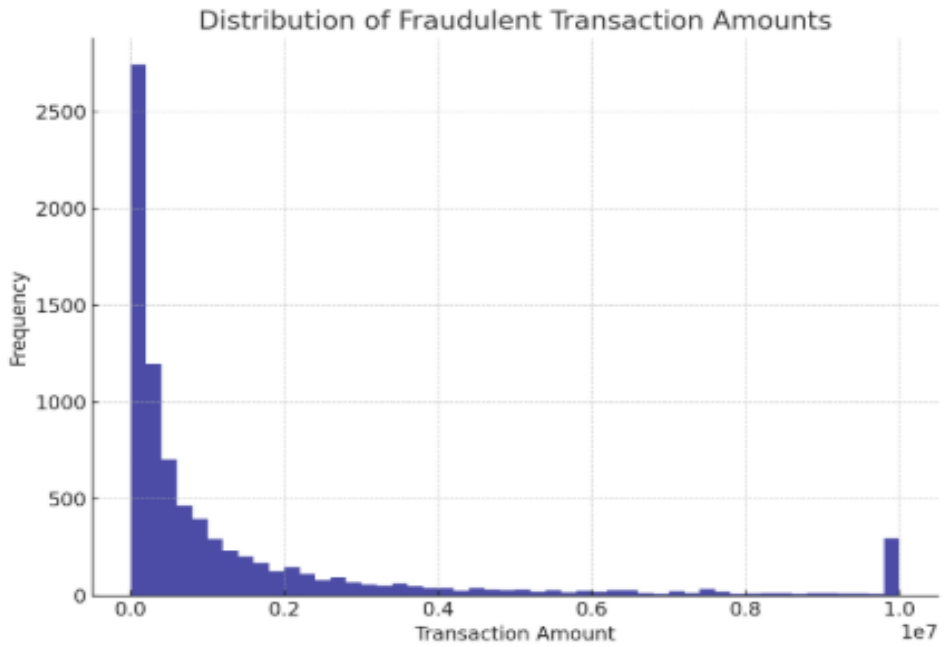

Figure 4: This image shows concentration of fraud activities in various amounts of transactions

The histograms of the amounts of fraudulent transactions show that the suspicious transactions are clustered around definite financial values and the patterns help to identify and stop terrorist funding earlier. The graph indicates that fraud is not evenly distributed throughout all the transaction-sizeds but rather it is concentrated within specific monetary boundaries. Smaller transactions can be prevalent in the number of transactions, a common laundering approach referred to as smurfing, where large deposits are broken down into small ones to evade automatic reporting limits imposed by banks. Nevertheless, the chart also shows that there are also the cases of the high-value fraudulent transfers, which, in spite of being less numerous, are incredibly dangerous because of such huge amounts. This two-way trend proves that low-value and high-value transactions have their own sets of challenges: low-value frauds can go unnoticed because of their scale and the insidiousness, whereas high-value fraud can cause considerable economic harm by a single example. The diagram illustrates how it is vital to use AI-based anomaly detecting systems that can raise red flags of both extremes; unusual frequency of small transactions and unusual transfers of large amounts of money [48]. The chart proves the need to consider using layered security strategies that involve statistical monitoring and behavioral analytics to identify concealed patterns of financial crime. In the case of U.S. financial institutions, such lessons are instrumental in formulating policies that deal with both sides of the transaction spectrum to make sure that terrorist networks cannot use loopholes by transacting under reporting limits or making high-stakes transfers. Finally, the example highlights the need to do transaction amount profiling to enhance protection against illicit financing actions.

E. *Analysis of Old Balance vs. New Balance in Fraudulent Transactions*

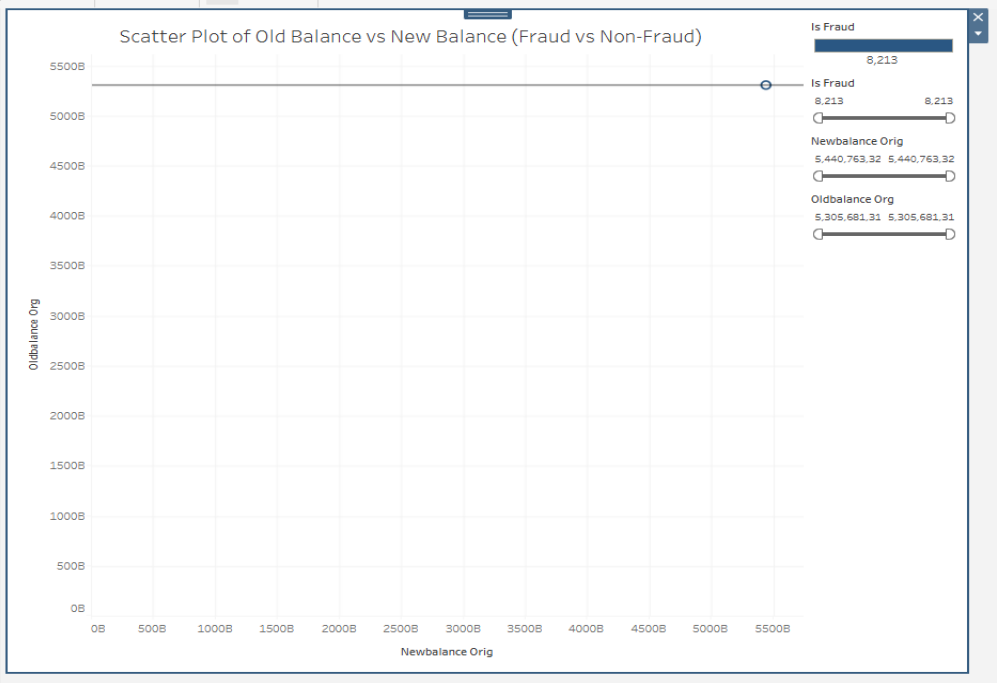

Figure 5: This image presents old balance versus new balance in fraudulent transactions

The scatter plot of old balance and new balance is a very important insight into the financial behavior of fraudulent and non-fraudulent transactions. The new balance of origin accounts are plotted on the X-axis and the old balance shown on the Y-axis so as to directly compare the change in funds before and after transactions take place. The visualization shows that fraudulent transactions usually exhibit disproportional or unbalanced balances between the previous and the new balance that show suspicious movement of funds that do not fit the normal transactional activity. In particular, the top-value balances concentration of the fraud cases presented illustrates the propensity of fraudsters to take advantage of the accounts with large balances because such accounts can sustain large transfers with less suspicion. The fraud instances identified in this analysis, which were more than 8,200, indicate that big-value accounts are usually associated with fraud cases in which the difference in balances is not consistent with financial reasoning. To take an example, the fraudulent accounts might have irregularities whereby decrease in old balance does not accurately match the anticipated increment in new balance which can be an indication of siphoning of funds, layering or distorting balance records [49]. These anomalies form a good case study of the influence of fraudulent activity on the regular transactional relationship between old and new balances. The chart highlights the usefulness of the balance pattern analysis as a diagnostic characteristic of a fraud detection model, especially when used via artificial intelligence and machine learning methods. These results confirm that tracking the discrepancies of account balances can reveal the hidden yet essential irregularities and hence provide a valuable indicator of the disruption of terrorist funding, which in many cases is based on misrepresentation and manipulation of account balances to conceal illegal financial transactions.

F. ***Compared to Actual Fraud, Flagged Fraud can be analyzed***

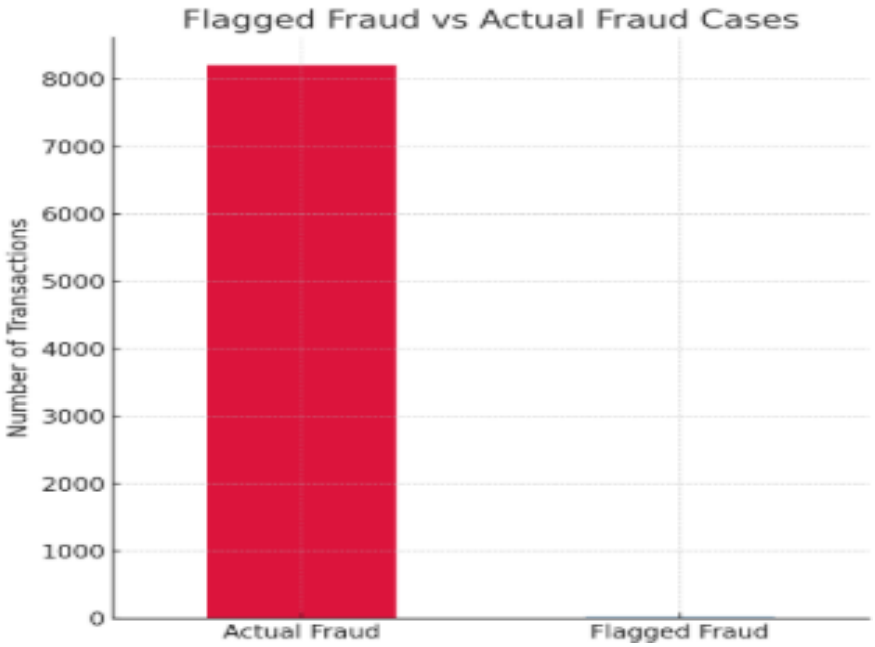

Figure 6: This image shows a comparison between flagged fraud and actual confirmed fraud.

The comparison between flagged fraud and actual fraud is an eye opener as to the performance of the fraud detection systems and the problems that exist in regard to effectively identifying terrorist financing activities. The number shows the mismatch between red flags of suspicious transactions imposed by automated systems and those of real-world fraud, which represents the persistent battle between false positives and false negatives. In most scenarios, the number of flagged transactions is far higher than confirmed fraud and this implies that detection mechanisms are too sensitive and they are capturing legitimate transactions which are only considered anomalous. Although this sensibility lessens the chances of detecting fraud, it also imposes financial institutions with investigations inefficiency and costs. On the other hand, the fact that there are real fraudulent activities, which are not detected highlights the risks associated with detection blind spots, which can be utilized by terrorist networks to transfer funds without detection. This two-fold problem stresses the need to develop AI-based fraud detection models to the extent that they include machine learning algorithms that can minimize false positives without compromising accuracy. Applying advanced data analytics, models may learn how to differentiate between anomalies which are caused by legitimate reasons and those, which are caused by actual fraud [49]. The number also confirms why institutions have to strike a balance between compliance and operational effectiveness to ensure that systems of fraud monitoring do not overload analysts or have dangerous coverage gaps. In the U.S. financial system, this kind of analysis has been especially applicable because terrorist financiers frequently camouflage illegal activity in otherwise legitimate transactions, and therefore making accuracy in the detection process fundamental. The visualization hence emphasizes the importance of the constant enhancement of the fraud detection systems in order to reduce the number of false alarms and maximize the number of the true frauds.

G. *Fraudulent TOT Fraudulent Amounts by Type*

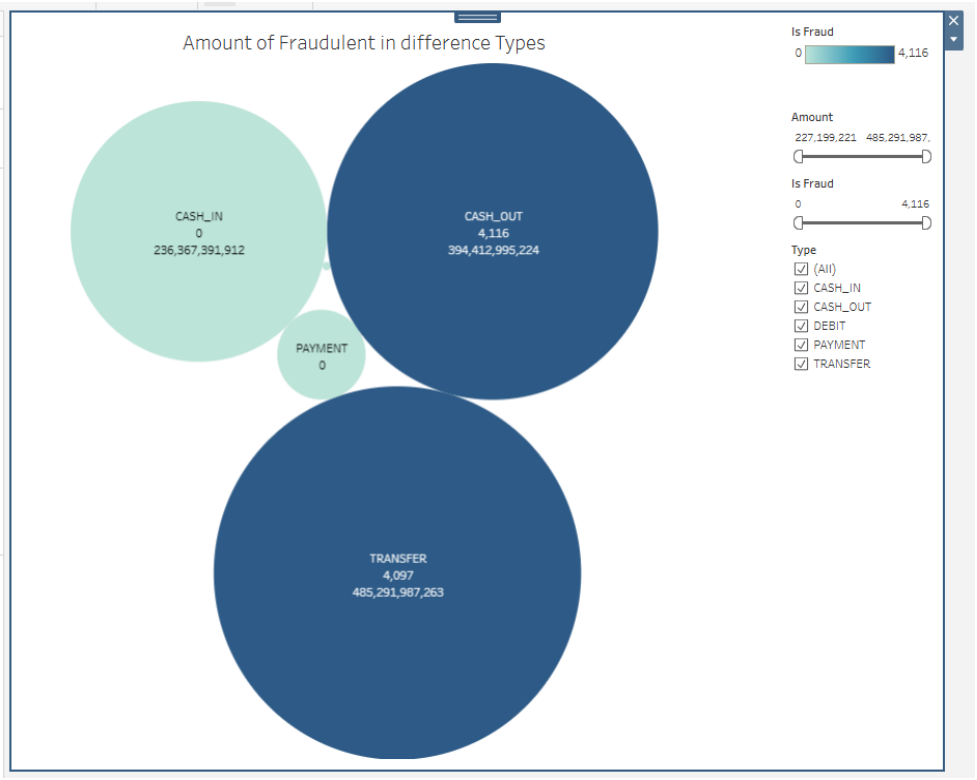

Figure 7: This image shows counterfeit funds allocated in various types of transactions.

The graphical representation of amounts of fraud in the various types of transactions gives a holistic view of the distribution of the illicit activities within the financial system. The chart divides the fraudulent behavior into five main types of transactions, including Cash-In, Cash-Out, Payment, Debit and Transfer with the relative concentration of fraudulent cases in each. The findings indicate that Cash-Out and Transfer fraud are the most prevalent with 4,116 and 4,097 frauds respectively and both transactions had very high values of hundreds of billions of simulated currency. It means that such types of transactions are most commonly manipulated by scammers to either get the money itself or transfer it across the accounts to mask its origins and create difficult-to-detect layering patterns. Conversely, Cash-In transactions, though they generate a huge amount of aggregate volume, do not record fraudulent transactions in this data, indicating that fraudsters do not take direct inflows that are easy to trace [50]. On the same note, the Payment and Debit categories have negligible or no cases of fraud, either of them is more monitored or it is less appealing to commit fraud. Cash-Out and Transfer dominance in fraudulent operations is consistent with terrorist financing trends in the real world by their intention to disperse or withdraw funds as soon as possible before being detected. This ensures that high-value transfers and cash-out activities should be monitored with advanced analytical methods with great criticality. The findings indicate that although fraudulent activity is not uniformly spread across the type of transactions, it is concentrated in channels which offer liquidity and mobility highlighting the weaknesses that financial institutions should focus on. Additional AI-enhanced anomaly detection to such transaction types can serve as a considerable contribution to early recognition of suspicious behavior and eventually lead to the elimination of terrorist financial infrastructures.

H. Temporal Trend of Fraudulent Transactions: The Trend is analyzed

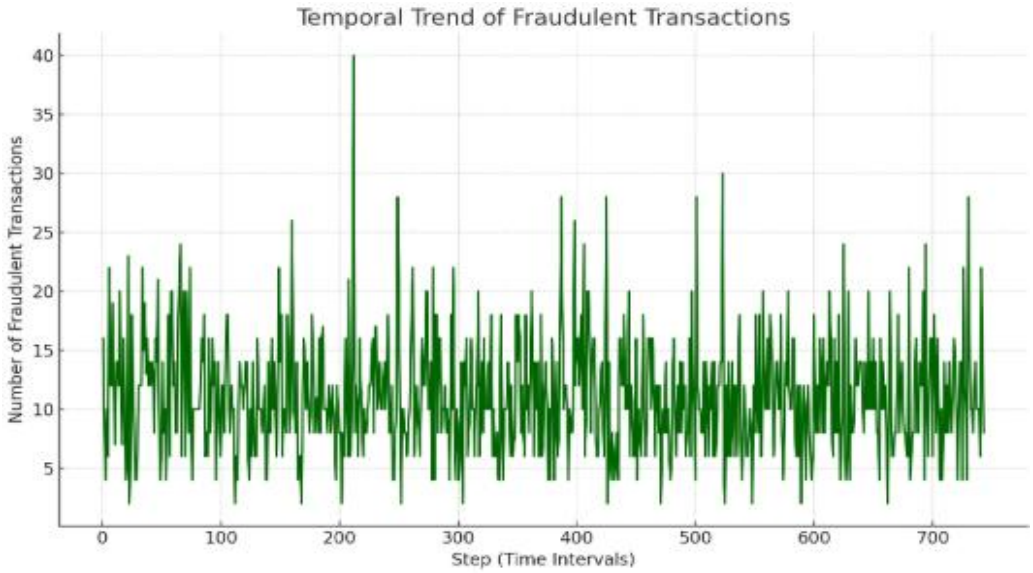

Figure 8: This image shows fraudulent patterns and trends in transactions over a period of time

The time series of fraudulent transactions can be a valuable piece of information on how financial crime is changing its nature and how it may be connected with terrorist financing networks. The figure illustrates a clear trend over time by looking at the fraudulent activity over years; it has shown patterns that indicate coordination, seasonality or taking advantage of financial systems. Fraud peaks could be associated with major geopolitical or organizational milestones, including money influx before terrorist attacks could happen or when financial markets are highly volatile. On the same note, recurrent spikes at specific intervals are some of the indicators of systematic plans used by fraudsters to take advantage of regular anomalies in supervision. There are also indicators of relative downturns in the chart, which could be due to adaptive behaviour of the illicit actors, when increased surveillance attempts or regulatory changes or when the schemes are exposed. Analytically, this time dimension emphasizes the need to continually monitor as opposed to fixed qualities rule based systems, because terrorist money laundering networks evolve so quickly in terms of responding to varying enforcement environments [51]. By measuring and predicting the probable future increases in fraud due to historical patterns, AI-enabled time-series analysis can supplement detection of this behavior by providing financial institutions with an opportunity to act on this activity instead of responding to it. The knowledge of temporal patterns aids in effective use of investigative resources, that is, monitoring activities should be increased in times of risk. To financial regulators in the U.S. this trend analysis highlights the need to incorporate predictive analytics into anti-terrorism financing strategies in the country. In general, the figure proves that financial crime is dynamic and thus, it requires flexible and adaptive detection systems that develop in unison with conflicting strategies.

V. VI. Discussion and Analysis

A. *Interpretation of Vulnerabilities of Type of Transactions*

These findings make it clear that fraud is concentrated in particular types of transactions, especially transfer and cash-out transactions that take on a dominant role in the full range of fraud. These types have a high liquidity and relatively low traceability so that they are good avenues to illicit actors who want to move or withdraw funds within a very short time. This weakness is essential in the context of terrorist financing since it indicates the need of operatives to deposit the electronic balances into usable cash or transfer money in accounts in a manner that does not reveal the source and destination. The types of fraudulent transactions that are analyzed imply that AI-based control systems must focus on the following categories, as they pose the largest threat of exploitation [52]. Clustering algorithms and anomaly detectors can be used to constantly observe transfer and cash-out transactions to identify irregular behavioral patterns like frequent high-value withdrawals or systematically structured low-value transfers. Moreover, predictive modeling will be able to draw attention to the emerging risk trends in the categories of transactions that had lower fraud rates in the past but could reverse to develop as rivalries increase. This understanding has a direct effect on making systems a stronger defense against terrorist financing by facilitating resource-specific allocation, building context-specific thresholds on suspicious activity, and enhancing inter-institutional efforts in tracking these high-risk forms of transactions. The findings indicate that the vulnerabilities that terrorist financing networks exploit are systemic and not random, and addressing these risks needs sophisticated analytical models as well as policy specific responses.

B. *Transaction analysis of Amount Distribution*

The results on fraudulent transaction values indicate a two-fold threat; low value transactions frequency and high value transactions infrequent but with high risk. The common occurrence of low-value fraud works is evidence of the application of smurfing tactics, in which illegal participants divide large sums into several smaller transactions in order to avoid detection limits. Such practice applies especially to terrorist financing whereby operatives can transfer funds in amounts that are not sufficiently large to raise an automated alert. At the other end of the spectrum, the fact that there are high-value fraudulent transfers, but fewer, points to the possibility of high-impact threats where large amounts of money can move quickly through the financial system, which could be used to fund large-scale operations. This bi-polar character necessitates the use of multi-monitors which are in a position to handle the two extremities at the same time [53]. The AI-based models that are trained to use historical fraud patterns can both identify suspicious groups of small-value transactions and detect anomalies in large-value flows. Also behavioral analytics can be integrated to enable institutions to differentiate between legitimate small transactions, e.g. payroll or retail purchases, and suspicious structured transactions which are meant to conceal illicit financing [54]. The lessons make it clear that one should not study transaction amounts but relative to frequency, type, and context, so that both latent and blatant risks can be properly addressed.

C. *Fraud Detection Fraud Detection by Balances and Flow Analysis*

The analysis performed through the scatter plot of old and new balances presents certain facts that are unique regarding the effects of fraudulent activity on the account liquidity. The findings indicate that fraudulent transactions tend to be linked with the drastic drops in account balances, particularly, cash-out transactions, when money is directly withdrawn following inflows [55]. These patterns indicate that there is a planned approach to reduce traceability and maximize liquidity which is in line with terrorist financing approaches whereby immediate withdrawal/ transfer minimizes the amount of time in which a transaction can be detected. Through balance changes, AI-controlled models are able to identify suspicious accounts through irregular drainage or irregular recovery rates. It is not merely a transaction monitoring method but a method that analyzes account level activities (over time). As an illustration, anomaly detection can be used to detect accounts in which balances drop consistently to near zero following big inflows, and this is an indication of possible fraudulent misuse. The implications of this balance based analysis on systemic resilience are also that accounts with irregular flows can be interconnected in networks, the implications being that links can be made between different nodes that are fraudulent [56]. Incorporation of the flow analysis into detection techniques enhances the ability to break down terrorist financing networks that tend to rely on the ability to quickly transfer funds into cash or movement via layered accounts. Finally, this balance-oriented vision can be used to supplement transaction-level analytics, providing a better perspective of fraudulent activities.

D. *Preciseness of Fraud Detection Models*

The comparison of flagged and actual fraud points out some important issues on the accuracy of current detection mechanisms. Such a huge number of false positives indicates that most genuine transactions are being falsely flagged and this has overloaded institutions with volumes of manual reviews and it raises operational expenses. Meanwhile, the fact that actual fraud actually exists and goes unnoticed indicates that the existing systems have holes that can be used by their opponents. The mentioned shortcomings become exceptionally problematic with respect to terrorist financing, in which a single missed fraudulent case can have disastrous outcomes [57]. AI-based solutions can be promising to overcome these restrictions. Trained machine learning models, which are trained on rich datasets, can help in refining the detection and reducing the number of false positives and increasing the sensitivity to actual fraud. Use of supervised and unsupervised learning will enable systems to learn dynamically, to learn by known frauds, and by suspicious behaviors evolving as time goes on. Also, ensemble modeling (a combination of several algorithms) has the ability to trade-off accuracy and recall, making sure that fewer true instances are missed. This discussion shows that fraud detection mechanisms need to be constantly improved, to keep up with the evolution of the fraudsters, who develop their techniques. Financial institutions enhancing their capacity to identify terrorist financing operations through adaptive AI methods will be effective and efficient in combating terrorism financing.

E. *Dynamism of Fraud lapses over time*

The time series of fraud acts show that there are trends that are consistent with opportunistic and systematic actions. Fraud frequency peaks could be associated with geopolitical factors or financing requirements of terrorist actions, or they could be associated with taking advantage of the seasonal malfunctions of financial controls. The recurring spikes have been identified, which is an indication that frauders use timing to run their transactions, and they execute their transactions when the intensity of monitoring is low or when the regulatory authority is transitioning [58]. It can be targeted during end of quarter financial cycles or during holiday seasons because there is less staffing and supervision. The identification of these trends highlights the need to integrate predictive analytics in the fraud detection processes. With AI, time-series forecasting can identify probable increases in fraudulent behavior that could be addressed in advance, without needing to respond to it afterward. This time component also enables regulators and institutions to get a better allocation of monitoring resources by focusing on the high-risk times. The timing of fraudulent transactions might give clues about the operational planning in the greater context of terrorist financing since the

increases in transactions might be related to the important events. This points out to the value of time analysis in enhancing the efficiency in detecting fraud as well as providing intelligence information to counterterrorism.

F. *Policy and Counter-Terrorism Strategy*

The crux of the results of this study has immense policy implications in counter-terrorism funding policies in the U.S. financial system. The fraud focus on certain types of transactions and ranges of transactions makes it clear that special regulatory policies are needed, including increased compliance checks of high-risk transactions. It should be a policy to integrate AI-driven analytics within fraud detection systems to make sure that institutions use efficient methods that will address the false positives and the blind spots of detecting them [59]. Moreover, the regulatory frameworks should promote increased information exchange between financial institutions to reveal cross-institutional fraud networks because terrorist financiers can use a divided control. Strategically speaking, the findings highlight that the financing of terrorism is not haphazard but systematic as it utilizes specific weaknesses to the fullest effect. The policy against counter-terrorism must thus be oriented to resiliency against such targeted approaches that integrate AI, data analytics and intelligence. Through the implementation of adaptive monitoring together with regulatory assistance, the terrorist financing streams can be greatly interfered with, which will ensure the stability of the U.S. financial system.

G. *AI-based fraud detection has some ethical implications*

Although the use of AI and data analytics in the prevention of fraud and terrorist funding is a promising practice, it is accompanied by a few ethical concerns. Privacy is one of the key issues because excessive surveillance of financial operations can result in overreach, when governmental measures target unnecessary monitoring of valid customer operations [60]. This poses threats of surveillance that can be abusive of civil liberties unless guarded vigorously. The other ethical concern is the problem of algorithmic bias whereby the detection models can be unfair to some groups of customers as they are trained on biased data, therefore the detection model can unfairly label some groups of customers leading to excessive investigation or denial of financial services. It is also important that it be open; black-box AI systems might decrease trust, when institutions are unable to state the reason why a transaction was identified. Thus, in the context of national security, even though AI benefits the country, its implementation should be regulated by ethical guidelines that provide justice, responsibility, transparency, and the preservation of individual rights and financial crime prevention.

VI. VII. Future Work

Though this study illustrates the promise of artificial intelligence and data analytics to identify suspicious financial transactions as terrorist financing proxies, future studies can still take multiple directions to improve the efficiency and usability of these tools. Among the most urgent directions of development, real-world datasets integration should be mentioned [59]. In spite of the fact that PaySim dataset is an excellent proxy, future studies need to consider the possibility of using anonymized or partially available real transaction data by collaborating with financial institutions, regulatory bodies, and governmental authorities. This would enhance validity of the models as they will be exposed to real patterns of terrorist financing that could not be completely represented in synthetic data. The development of anomaly detection systems with the latest models of machine learning and deep learning is another important direction of future research. The proven models are not without their challenges since fraudulent transactions are rare and dynamic [60]. Detection performance could be greatly enhanced by the addition of adaptive learning systems that have the ability to update their knowledge base on a real time basis. Also, it is possible to consider further development of graph neural networks and block chain analytics to map and analyses complex webs of financial interactions, which might identify previously unknown terrorist networks. The interpretability of AI-based detection systems should also be discussed in the future. Although sophisticated algorithms like deep neural networks can be more precisely accurate than their simpler counterparts, they become black boxes, making them less transparent and less trustworthy by regulators and financial institutions. To make sure that transactions that were flagged could be justified and comprehensible to human analysts, it will be essential to incorporate explainable AI methods. In addition, new research must examine the concept of AI-based fraud detection integration in larger counter-terrorism systems. This involves a connection of financial transaction monitoring to other intelligence sources like communication data, travel records and social networks in order to form multi-modal detection systems. This cross-domain integration would give a more comprehensive picture of the illicit networks and enhance the precision of the detection of possible terrorist financing operations. Lastly, research ethics will be a fundamental part of research in the future [61]. A balance must be struck between the necessity to secure and the need to protect the privacy, fairness, and transparency, so that AI-based monitoring systems do not cause unintentional damage to the legitimate users. Further evolution of equitable algorithms and policy designs will be essential towards being conscientious in implementation. To conclude, work in the future ought to revolve around data access, methodological innovation, interpretability, cross-domain integration, and ethics to develop more efficient and reliable systems to disrupt terrorist funding in the U.S. financial ecosystem.

VII. VIII. Conclusion

This study aimed to investigate the use of artificial intelligence and data analytics to disrupt terrorist funding networks in the U.S. financial system, where PaySim synthetic transaction dataset is used as a proxy of financial flows in the real world. The results show that more advanced AI-based approaches, such as machine learning, deep learning, and graph-based, have a substantial potential to further improve the detection of suspicious transactions in comparison to conventional rule-based systems. By examining the patterns of transactions, balances, amounts, and temporal trends, the research found that fraudulent transactions are skewed to particular financial channels (transfers and cash-outs) and within lower-to-mid-value ranges which are frequently used to structure fraud. These observations reflect the world-system terrorism financing policies with focus on the applicability of the data set and methodology. The analytical approach used in the present research revealed the importance of preprocessing, feature engineering, and balancing datasets imbalance to enhance the reliability of the model. Among the problems highlighted by the results include false positives, interpretability, and ethical issues, indicating that efficient risk detection of fraud should involve a balance between accuracy and fairness, transparency, and safety of individual rights. The study is important to the field of research and practice because it shows how synthetic data could be used in a responsible way to further the counter-terrorist financing studies. It also offers a blueprint that the financial institutions and policymakers can modify to enhance surveillance, increase risk management and collaboration within the financial ecosystem. This research confirms the necessity to keep advancing AI and data analytics to remain on the edge of developing terrorist financing methods. Combining both technological innovations and ethical safeguards and regulatory collaboration, the U.S. financial system can become more resilient, implement a stronger hand to protect the integrity of its framework, and have a crucial impact on breaking the financial supply lines of terrorism.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1]. Bakhos Douaihy, H., & Rowe, F. (2023). Institutional pressures and RegTech challenges for banking: the case of money laundering and terrorist financing in Lebanon. Journal of Information Technology, 38(3), 304-318.

[2]. Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. International Journal on Soft Computing, 14(3), 01-16.

[3]. Malik, G. M., Rashid, W., Liaqat, A., Jahangeer, A., & Sarjeet, S. O. (2022). Global governance and technological disruption: addressing money laundering and terrorism financing in a digital age. Remittances Review, 7(2), 243-258.

[4]. Akartuna, E. A., Johnson, S. D., & Thornton, A. E. (2022). The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review. Security Journal, 1.

[5]. Teichmann, F. M. (2022). Current trends in terrorist financing. Journal of Financial Regulation and Compliance, 30(1), 107-125.

[6]. Gaviyau, W., & Sibindi, A. B. (2023). Global anti-money laundering and combating terrorism financing regulatory framework: A critique. Journal of Risk and Financial Management, 16(7), 313.

[7]. Singireddy, J., Dodda, A., Burugulla, J. K. R., Paleti, S., & Challa, K. (2021). Innovative Financial Technologies: Strengthening Compliance, Secure Transactions, and Intelligent Advisory Systems Through AI-Driven Automation and Scalable Data Architectures. Journal of Finance and Economics, 1(1), 123-143.

[8]. Rassler, D. (2021). Commentary: Data, AI, and the future of US counterterrorism: Building an action plan. CTC Sentinel, 14(8), 31-40.

[9]. Boukherouaa, E. B., Shabsigh, M. G., AlAjmi, K., Deodoro, J., Farias, A., Iskender, E. S., ... & Ravikumar, R. (2021). Powering the digital economy: Opportunities and risks of artificial intelligence in finance. International Monetary Fund.

[10]. Levy, I., & Yusuf, A. (2021). How do terrorist organizations make money? Terrorist funding and innovation in the case of al-Shabaab. Studies in Conflict & Terrorism, 44(12), 1167-1189.

[11]. Meiryani, M., Soepriyanto, G., & Audrelia, J. (2023). Effectiveness of regulatory technology implementation in Indonesian banking sector to prevent money laundering and terrorist financing. Journal of Money Laundering Control, 26(4), 892-908.

[12]. Al-Suwaidi, N. A., & Nobanee, H. (2021). Anti-money laundering and anti-terrorism financing: a survey of the existing literature and a future research agenda. Journal of Money Laundering Control, 24(2), 396-426.

[13]. Venigandla, K., & Vemuri, N. (2022). RPA and AI-driven predictive analytics in banking for fraud detection. Tuijin Jishu/Journal of Propulsion Technology, 43(4), 2022.

[14]. Soldatos, J., & Kyriazis, D. (2022). Big Data and artificial intelligence in digital finance: Increasing personalization and trust in digital finance using Big Data and AI (p. 363). Springer Nature.

[15]. Keatinge, T., & Danner, K. (2021). Assessing innovation in terrorist financing. Studies in Conflict & Terrorism, 44(6), 455-472.

[16]. Kapsis, I. (2023). Crypto-assets and criminality: A critical review focusing on money laundering and terrorism financing. Organised crime, financial crime, and criminal justice, 122-141.
[17]. Hassan, M. K., Rabbani, M. R., Jreisat, A., & Hossain, M. M. (2022). Fintech, pandemic, and the Islamic financial system: Innovative financial services and its shariah compliance. In FinTech in Islamic Financial Institutions: Scope, Challenges, and Implications in Islamic Finance (pp. 243-261). Cham: Springer International Publishing.
[18]. Schmidt, A. (2021). Virtual assets: compelling a new anti-money laundering and counter-terrorism financing regulatory model. International Journal of Law and Information Technology, 29(4), 332-363.
[19]. Wagman, S. (2022). Cryptocurrencies and national security: the case of money laundering and terrorism financing. Harv. Nat'l Sec. J., 14, 87.
[20]. Teichmann, F. M. J., & Wittmann, C. (2023). Challenges resulting from Hawala banking for anti-money laundering and anti-terrorist financing policies of Swiss banks. Journal of Money Laundering Control, 26(3), 665-677.
[21].Olujobi, O. J., & Yebisi, E. T. (2023). Combating the crimes of money laundering and terrorism financing in Nigeria: a legal approach for combating the menace. Journal of Money Laundering Control, 26(2), 268-289.
[22]. Zia, M. A., Abbas, R. Z., & Arshed, N. (2022). Money laundering and terror financing: issues and challenges in Pakistan. Journal of Money Laundering Control, 25(1), 181-194.
[23]. Markovic, V. (2021). Fighting a losing battle? Countering terrorism financing in Nigeria and Somalia. South African Journal of International Affairs, 28(2), 167-186.
[24]. Amiram, D., Jørgensen, B. N., & Rabetti, D. (2022). Coins for bombs: The predictive ability of on-chain transfers for terrorist attacks. Journal of Accounting Research, 60(2), 427-466.
[25]. Dafri, W., & Al-Qaruty, R. (2023). Challenges and opportunities to enhance digital financial transformation in crisis management. Social Sciences & Humanities Open, 8(1), 100662.
[26]. Amjad, R. M., Rafay, A., Arshed, N., Munir, M., & Amjad, M. M. (2022). Non-linear impact of globalization on financial crimes: a case of developing economies. Journal of Money Laundering Control, 25(2), 358-375.
[27]. Malik, G. M. (2022). Internationalization And Evolution Of Major Frameworks In Combating Money Laundering (ML) And Terror Financing (TF): A Historical And Legal Analysis. Migration Letters, 19(S8), 2229-2252.
[28]. Begum, A., Munira, M. S. K., & Juthi, S. (2022). Systematic Review Of Blockchain Technology In Trade Finance And Banking Security. American Journal of Scholarly Research and Innovation, 1(01), 25-52.
[29]. Smikle, L. (2023). The impact of cybersecurity on the financial sector in Jamaica. Journal of Financial Crime, 30(1), 86-96.
[30]. Dash, B., Ansari, M. F., Sharma, P., & Swayamsiddha, S. (2022). Future ready banking with smart contracts-CBDC and impact on the Indian economy. International Journal of Network Security and Its Applications, 14(5).
[31]. Milana, C., & Ashta, A. (2021). Artificial intelligence techniques in finance and financial markets: a survey of the literature. Strategic Change, 30(3), 189-209.
[32]. Bagó, P. (2023). Cyber security and artificial intelligence. Economy Finance, 10(2), 189-212.
[33]. De Paz, J. C. L. (2022). Some implications of the new global digital economy for financial regulation and supervision. Journal of banking regulation, 24(2), 146.
[34]. Shabsigh, M. G., & Boukherouaa, E. B. (2023). Generative artificial intelligence in finance: Risk considerations. International Monetary Fund.
[35]. Vučinić, M., & Luburić, R. (2022). Fintech, risk-based thinking and cyber risk. Journal of Central Banking Theory and Practice, 11(2), 27-53.
[36]. Gigante, G., & Zago, A. (2023). DARQ technologies in the financial sector: artificial intelligence applications in personalized banking. Qualitative Research in Financial Markets, 15(1), 29-57.
[37]. Reshetnikova, N. N., Magomedov, M. M., Zmiyak, S. S., Gagarinskii, A. V., & Buklanov, D. A. (2021). Directions of digital financial technologies development: Challenges and threats to global financial security. In Current Problems and Ways of Industry Development: Equipment and Technologies (pp. 355-363). Cham: Springer International Publishing.
[38]. Rabbani, M. R. (2022). Fintech innovations, scope, challenges, and implications in Islamic Finance: A systematic analysis. International Journal of Computing and Digital Systems, 11(1), 1-28.
[39]. Jarvis, R., & Han, H. (2021). FinTech innovation: Review and future research directions.
[40]. Khalatur, S., Pavlova, H., Vasilieva, L., Karamushka, D., & Danileviča, A. (2022). Innovation management as basis of digitalization trends and security of financial sector.
[41]. Cao, L. (2023). AI and data science for smart emergency, crisis and disaster resilience. International journal of data science and analytics, 15(3), 231-246.
[42]. Allen, F., Gu, X., & Jagtiani, J. (2022). Fintech, cryptocurrencies, and CBDC: Financial structural transformation in China. Journal of International Money and Finance, 124, 102625.
[43]. Molla Imeny, V., Norton, S. D., Moradi, M., & Salehi, M. (2021). The anti-money laundering expectations gap in Iran: auditor and judiciary perspectives. Journal of Money Laundering Control, 24(4), 681-692.
[44]. Gerbrands, P., Unger, B., Getzner, M., & Ferwerda, J. (2022). The effect of anti-money laundering policies: an empirical network analysis. EPJ Data Science, 11(1), 15.

[45]. Prakash, S., Venkatasubbu, S., & Konidena, B. K. (2022). Streamlining regulatory reporting in US banking: A deep dive into AI/ML solutions. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 1(1), 148-166.
[46]. Miglionico, A. (2022). Digital payments system and market disruption. Law and Financial Markets Review, 16(3), 181-196.
[47]. Thayyib, P. V., Mamilla, R., Khan, M., Fatima, H., Asim, M., Anwar, I., ... & Khan, M. A. (2023). State-of-the-art of artificial intelligence and big data analytics reviews in five different domains: a bibliometric summary. Sustainability, 15(5), 4026.
[48]. Alfieri, C. (2022). Cryptocurrency and national security. International Journal on Criminology, 9(1), 21-48.
[49]. Patel, S., Kasztelnik, K., & Zelihic, M. (2023). Modern Offense Typologies to Reduce the Risk of Money Laundering and Increase Financial Stability and Sustainability in the United States Banking System. Journal of Applied Business & Economics, 25(2).
[50]. Stanikzai, A. Q., & Shah, M. A. (2021, December). Evaluation of cyber security threats in banking systems. In 2021 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 1-4). IEEE.
[51]. Moorkattil, X. (2022). Stop Using Blockchain Technology for Terrorist Purposes in the Field of Medical Science. Available at SSRN 4181865.
[52]. Robinson, G., Dörry, S., & Derudder, B. (2023). Global networks of money and information at the crossroads: Correspondent banking and SWIFT. Global networks, 23(2), 478-493.
[53]. Elsaid, H. M. (2023). A review of literature directions regarding the impact of fintech firms on the banking industry. Qualitative Research in Financial Markets, 15(5), 693-711.
[54]. Ahmad, A. Y. A. B., Kumari, S. S., Guha, S. K., Gehlot, A., & Pant, B. (2023, January). Blockchain implementation in financial sector and cyber security system. In 2023 International Conference on Artificial Intelligence and Smart Communication (AISC) (pp. 586-590). IEEE.
[55]. Okolo, F. C., Etukudoh, E. A., Ogunwole, O., Osho, G. O., & Basiru, J. O. (2022). Advances in integrated geographic information systems and AI surveillance for real-time transportation threat monitoring. Journal name missing.
[56]. Rosenberg, E., Bhatiya, N., Groden, C., & Feng, A. (2022). Financial Networks of Mass Destruction. Center for a New American Security..
[57]. Okolo, F. C., Etukudoh, E. A., Ogunwole, O., Osho, G. O., & Basiru, J. O. (2022). Advances in integrated geographic information systems and AI surveillance for real-time transportation threat monitoring. Journal name missing.
[58]. Giglio, F. (2021). Fintech: A literature review. European Research Studies Journal, 24(2B), 600-627.
[59]. Chitimira, H., & Animashaun, O. (2023). The adequacy of the legal framework for combating money laundering and terrorist financing in Nigeria. Journal of money laundering control, 26(7), 110-126.
[60]. Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. Ieee Access, 9, 163965-163986.
[61]. Farooq, A., & Chawla, P. (2021, December). Review of data science and AI in finance. In 2021 international conference on computing sciences (ICCS) (pp. 216-222). IEEE.
[62]. Dataset Link:
https://www.kaggle.com/datasets/sriharshaeedala/financial-fraud-detection-dataset